ETH Zürich, D-INFK
HS 2017, 6. November 2017

Prof. Ueli Maurer
Marta Mularczyk

Diskrete Mathematik

Exercise 8

8.1 Diffie-Hellman

a) ($\star$ $\star$) Since Alice can add much faster than she can multiply, she proposes to execute the Diffie-Hellman protocol using the group $\langle \mathbb{Z}_n; \oplus \rangle$ with a generator $g \in \mathbb{Z}_n$. Describe the messages exchanged between Alice and Bob in this case. Show that this protocol is insecure, that is, describe a way in which Eve, who eavesdrops on all exchanged messages, can recover the secret key.

b) ($\star$ $\star$ $\star$) Since, by subtask a), the Diffie-Hellman protocol is insecure in the group $\langle \mathbb{Z}_n; \oplus \rangle$ and by Theorem 5.7 every cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n; \oplus \rangle$, Bob concludes that the protocol is insecure in every cyclic group. Is he right?

8.2 Algebras ($\star$ $\star$)

For each of the following algebras, decide whether it is a monoid, a group or neither. In case it is a monoid or a group, decide whether it is abelian. Justify your answers.

a) $\langle \mathbb{Z}; \star \rangle$, where $\star$ is defined by $a \star b := a^2 + b^2$ for any $a, b \in \mathbb{Z}$.

b) $\langle \mathcal{P}(X); \cup \rangle$, where X is a non-empty finite set.

8.3 Facts about groups ($\star$ $\star$) *(5 Points)*

In this exercise you are not allowed to use lemmas from the lecture notes (especially, Lemma 5.3).

Let $\langle G; *, \widehat{\ }, e \rangle$ be a group. Prove the following fact:

a) Show that in the group axioms it is sufficient to request that there exists a right neutral element. That is, show that the group axiom **G2** follows from the axioms **G1**, **G2'** and **G3**, where

G2': There exists a (right neutral) element $e \in G$ such that $a * e = a$ for all $a \in G$.

(2 Points)

Let $a, b, c \in G$. Prove further that:

b) $\widehat{a * b} = \widehat{b} * \widehat{a}$ *(2 Points)*

c) $a * b = a * c \;\Rightarrow\; b = c$ *(1 Point)*

8.4 Structure of groups ($\star\,\star$)

a) Let $\langle G; *, \widehat{\ }, e\rangle$ be a group. Show that if for all $a \in G$, we have $a * a = e$, then G is abelian.

b) Let $\langle G; *, \widehat{\ }, e\rangle$ be a group. Prove that for any set $H \subseteq G$, we have that H is a subgroup of G if and only if $H \neq \varnothing$ and $a * \widehat{b} \in H$ for all $a, b \in H$.

8.5 Symmetries of a cube

A sofa in the shape of a cube stands in the corner of a room. The corners of the sofa are marked with numbers from 0 to 7.

a) ($\star$) In how many ways can the sofa be placed in the corner?

Now one can take the sofa from the corner, rotate it in an arbitrary way and place it back in the corner. We distinguish two rotations b_1 and b_2 if the position of the sofa is different after the rotation b_1 and after b_2. Let R denote the set of such different rotations.

b) ($\star\,\star$) Determine $|R|$. Is it possible to describe each element of R as a rotation around a single axis? (For different elements the axes can be different.)

c) ($\star\,\star$) Let $b_2 \circ b_1$ denote applying to the sofa first the rotation b_1 and then the rotation b_2. Is $\langle R; \circ\rangle$ a group?

d) ($\star$) Is $\circ$ commutative?

Due on 13. November 2017.
Exercise 8.3 will be corrected.